Military Certification: A Practitioner's View

Peggy Wright

Designated Alteration Station

Authorized Representative (AR) – Software

Boeing Integrated Defense Systems – Wichita

FAA Certification of Military Aircraft Overview

- How It Is Done
- State of the Art
- Challenges

BOEING®

How It Is Done - The Balancing Act

- Different Fundamental Focus

FAA focus is **Safety**/Function

Military focus is **Mission**/Safety

How It Is Done - Ultimate Airworthiness Authority

Civil Oversight = FAA

Military Oversight = Military Customer

How Can Military Aircraft Achieve FAA Certification?

- Civil Certification of civil systems is performed as usual
- Military mission systems are "capped and stowed or the certification cites "provisions only"
- Excluded systems must be shown not to interfere with civil system operation.
  - How, if capped and stowed?
- Further, for a partitioned, multi-function box, how can you turn off or ignore a military software function in the box?

BOEING®

Value of FAA Certification

- Safety
- Reliability
- International Acceptance
- Reduced Redundancy of Standards
  - Adoption of Civil Standards eliminates the need for DoD to maintain its own standards

BOEING®

How It Is Done - Proposals/Estimates

- Military contractors may fail to incorporate the certification effort when developing
  - Proposals
  - Estimates
  - Statements of Work (SOW)
  - Contracts

How It Is Done - Procurement

- Military integrators and subcontractors are unaccustomed to considering the cost and schedule impact of
  - Data deliveries for certification
  - Review and approval cycles
  - In-process audits
  - Conformity process
  - FAA test witnessing
  - Software conformity review
  - Scope of data retention required for the life of the aircraft

Military Procurement Problems Regarding Certification

- Military procurement processes are prone to underestimate or omit certification requirement compliance effort in
  - SOWs
  - Contracts
  - Deliverable Approvals
- Results in discord between program and cert authority

How It Is Done - Safety Analysis

- Military contractors are not accustomed to the SAE ARP 4754/4761 safety analysis processes.
- Military contractors sometimes perform safety analysis late in the product lifecycle, whereas the FAA expects the safety analysis to
  - provide input on design assurance levels early
  - be consulted throughout the software assurance process.
- Military software suppliers are not accustomed to the granularity or level of oversight corresponding to 5 levels of software criticality.

- **The safety process must be permitted to drive requirements**.

BOEING®

How It Is Done - Quality Assurance (QA)

- The quality process may not be as strong or as comprehensive as is needed for the FAA.
- DO-178B requires involvement of QA throughout the lifecycle, especially for Level A, with
  - Independence
  - Authority to drive process change
- Military programs may not give QA the level of independence that the FAA expects.
  - QA may report to the program manager
  - QA may not have the independence to require process changes

How It Is Done - Configuration Management (CM)

- Configuration control varies
  - Source code – rigorously controlled
  - Requirements and design – less rigorously controlled
  - Test scripts and test cases – even less carefully controlled
- Concept of varying levels of control (configuration control vs. change control) is absent
- Authority to drive changes varies
  - Who has a voice on the change control board?
    - Engineering, QA, Management, Safety
  - Who has the authority to approve changes?
  - How are changes tracked and controlled?
- Which artifacts are retained, by whom, and for how long?

Verification

- Military does require verification throughout the lifecycle
- Military still relies on Independent Verification and Validation (IV&V) performed by a separate group from the system developer
- Military still tends to rely on large design review meetings as a means of meeting verification requirements
- Detailed reviews of all artifacts are needed throughout the lifecycle, with evidence retained in CM

Multiple Companies

- Teaming is today's business paradigm
  - The problem is there is seldom a team devoted solely to the integrated product, with the result that when cert authorities ask questions, there may be a lot of finger pointing, followed by long tedious meetings between contracts personnel to determine who is responsible for providing the answers.
  - Sometimes one company writes the software plans, and its subcontractor intends to follow those plans, but simply does not have the infrastructure in place either to make that feasible, or even to detect whether it is happening.

-- Sometimes an expert subcontractor or consultant is hired that makes the program shine.

Certification Liaison

- When the design assurance processes break down, it falls to the DER/AR to guide the project team as well as to find compliance.
- A new trend is for a military integrator to ask its suppliers to provide findings of compliance along with their products.
  - This only works to a point
  - System integration testing and compliance findings are still required
- Sometimes DO-178B is called out by the customer as a contractual requirement for a military system, but there is no requirement for FAA or designee oversight

State of the Art

- Military Certification is a balancing act

State of the Art – Proposals/Estimates

+ Military is requiring contractors and subs to follow FAA certification standards, including DO-178B for military software

- Such a military contract may still not require any oversight from the FAA or designees to assure this has been accomplished
  - How will they know they got what they paid for?
  - Where is the objective evidence?

BOEING®

State of the Art – Military Contractors

+ Are learning the hard lessons of the cost and schedule impact of certification data deliveries, conformity, etc.

- Haven't fully integrated the planning for these required certification activities into their processes

State of the Art - Safety

+ Functional Hazard Analysis and Safety Assessment are being performed earlier in military programs

- Safety organizations are still not fully empowered to drive design changes

State of the Art - QA

+ Learning to take a stronger role throughout the lifecycle by demanding greater independence, a seat on the change control board, authority to require process conformance, process change, etc.

- Not comprehensive enough yet – much is left to DER/AR to oversee – QA must be a partner in the engineering process

State of the Art - CM

+ Strong CM processes are in place for some of the data,
  especially source code

- More detailed lists are needed of what data requires configuration management, and of what level of control is required (see DO-178B CC1 and CC2)
  - Include type design data, lifecycle data, lifecycle environment, tools, etc.

State of the Art - Verification

+ Military understands the value of independent verification (see IV&V)

- Military programs rely on large design review meetings
  - Smaller, more detailed internal review meetings are also needed.
  - Checklists for verification reviews are needed,
    - Records should be retained.
    - Discrepancies should be tracked to closure.

State of the Art – Multiple Companies Building One System

+ Military companies are trying to adapt their processes to accommodate IMA systems and FAA certification

- Careful oversight is required from a central system integration team
  - Create detailed verification plan that addresses all requirements regarding functionality, system timing, throughput, data & control coupling, etc.
  - Create detailed responsibility plan with corresponding contracts

***This is not unique to military programs!**

BOEING®

State of the Art – Cert Liaison

+ Military customers are requiring FAA standards from their suppliers for GATM, etc.
- Requiring FAA processes without assuring FAA or designee oversight is hazardous.
    - Give cert authorities a break – their time and resources are limited too.
    - MCO is working to leverage the Military Qualification process to facilitate FAA acceptance where appropriate

BOEING®

Challenges for Military Certification Programs

- **Procurement**
  - Incorporate certification personnel at the proposal stage
  - Incorporate certification activities in proposals, SOWs, contracts, data delivery lists, and schedules
- **Safety**
  - Follow SAE ARP 4754/4761 process
  - Initiate early in program
  - Expect safety to drive program requirements
- **Verification**
  - Perform structural coverage testing, data and control coupling analysis
  - Verify the system DOES NOT do what it SHOULD NOT do (robustness)
- **Certification Liaison**
  - Communicate early and often.
  - Negotiation to determine the cert basis occurs early in a program.
  - There can be no negotiation later regarding compliance with CFRs.
  - FAA cannot worry about cost or schedule.

BOEING®

Bottom Line

- Everyone believes in their hearts that what they are already doing is "good enough".
- We need to study and understand each other's processes in greater detail.
- Acknowledgement must come from both sides that we are ALL working toward the same goal: **Effective Software for Safety of Flight**

BOEING®